Автоматизация в промышленности 2023. №07
www.avtprom.ru

DOI: 10.25728/avtprom.2023.07.03

В.В. Покусов (КАИБ)

Метод синтеза модульной архитектуры организационно-технической системы класса «ИСЗИ»

Исследована абстрактная интегрированная система защиты информации (ИСЗИ) на предмет ее внутренних взаимосвязей и взаимодействий, снижающих итоговую эффективность ввиду отсутствия их универсальности. Рассмотрен пример многоэтапного деструктивного воздействия на корпоративную информационную систему (КИС), «вскрывающий» основное противоречие, возникающее при построении современных ИСЗИ. Предложен метод формирования модулей ИСЗИ путем категориального деления на три пары – Данные vs Функция, Человек vs Машина и Анализ vs Синтез. Синтезирована схема, гипотетически описывающая все информационно-техническое взаимодействие модулей ИСЗИ, особенностью которой является синхронизация элементов модели защиты с моделями внешних ИСЗИ, что позволяет поддерживать Best Practices.

Ключевые слова: корпоративная информационная система, многоэтапное деструктивное воздействие, интегрированная система защиты информации, модульная архитектура, метод синтеза, категориальной деление, информационно-техническое взаимодействие.

Покусов Виктор Владимирович *– заведующий лабораторией компьютерной криминалистики и исследования*
программного обеспечения Национального института развития в сфере обеспечения информационной безопасности, Председатель Казахстанской ассоциации информационной безопасности (КАИБ), Алматы, Казахстан.

Список литературы

1. Буйневич М.В., Покусов В.В., Ярошенко А.Ю., Хорошенко С.В. Категориальный подход в приложении к синтезу архитектуры интегрированной системы обеспечения безопасности информации / // Проблемы управления рисками в техносфере. 2017. № 4 (44). С. 95-102.
2. De Donno M., Giaretta A., Dragoni N., Spognardi A. A taxonomy of distributed denial of service attacks // International Conference on Information Society (i-Society). 2017. PP. 100-107.
3. Покусов В.В., Матвеев А.В., Максимов А.В. К вопросу о методах и средствах интеграции подсистем защиты информации в информационной системе // В сб.: Пожарная безопасность: современные вызовы. Проблемы и пути решения. Материалы Международной научно-практической конференции / Составители Т.В. Мусиенко, В.А. Онов, Н.В. Федорова. 2020. С. 104-106.
4. Андрианова В.Д., Покусов В.В. Состав интегрированной системы безопасности: аналитический обзор Топ-20 // Молодежная научная школа кафедры «Защищенные системы связи». 2020. Т. 1. № 1 (1). С. 80-85.
5. Li W., Huang J., You W. Attack modeling for Electric Power Information Networks // International Conference on Power System Technology. 2010. PP. 1-5.
6. Maciel R., Araujo J., Dantas J., Melo C., Guedes E., Maciel P. Impact of a DDoS attack on computer systems: An approach based on an attack tree model // Annual IEEE International Systems Conference (SysCon). 2018. PP. 1-8.
7. Jithish J., Sankaran S. Securing networked control systems: Modeling attacks and defenses IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). 2017. PP. 7-11
8. Ackerman D., Mehrpouyan H. Modeling human behavior to anticipate insider attacks via System Dynamics // Symposium on Theory of Modeling and Simulation (TMS-DEVS). 2016. PP. 1-6.a
9. Покусов В.В. Формат протокола универсального информационно-технического взаимодействия для системы обеспечения ИБ «УИТВ–ИСЗИ» // Телекоммуникации. 2019. № 9– С. 33-40.
10. Ramachandran M., Chang V. Recommendations and Best Practices for Cloud Enterprise Security // IEEE 6th International Conference on Cloud Computing Technology and Science. 2014. PP. 983-988.
11. Swafford C., Doan D., Nagl M., Sullivan P. Electrical Injury Drills: Approaches, Information, and Best Practices // IEEE Industry Applications Magazine. 2018. Vol. 24. No. 3. PP. 12-20.

Pokusov V.V. Synthesizing modular architecture for integrated information security systems

The paper investigates an abstract integrated information security system (IISC) for establishing its internal interrelations and interactions which decrease the system's overall efficiency owing to the lack of their versatility. A case of a multistage destructive impact on a corporate information system is examined. It shows the basic contradiction underlying the design of present-day IISC. A method for developing IISC modules is proposed. It decomposes the synthesis task into three categorial pairs: Data vs. Function, Human Individual vs. Machine, and Analysis vs. Synthesis. A scheme is synthesized, which describes hypothetically the overall information technology interrelation of IISC modules. This interaction synchronizes security model's elements with external IISC models in compliance with the best practices.

Keywords: corporate information system, multistage destructive impact, integrated information security system, modular architecture, synthesis method, categorization, informational technology interaction.